

GeekBrains

Урок 4 Видео 1

Криптография

Обзор MAC и HMAC

В этом видео

1. MAC
2. Виды MAC
3. Устройство HMAC

Зачем нужен Message Authentication Code (MAC)?

Предоставляет возможность подтвердить, что сообщение не было изменено

Позволяет быть уверенным, что сообщение получено от лица, знающего секретный ключ

MAC — алгоритм, который принимает на вход сообщение и ключ, а на выходе производит имитовставку (tag), которая позволяет гарантировать целостность сообщения и тот факт, что сообщение отправлено лицом, знающим ключ



Наивная реализация MAC

Одной из небезопасных и распространенных реализаций MAC является $t = H(k \| m)$, где t - MAC, H - хеш-функция, k - ключ, m - сообщение



Виды MAC

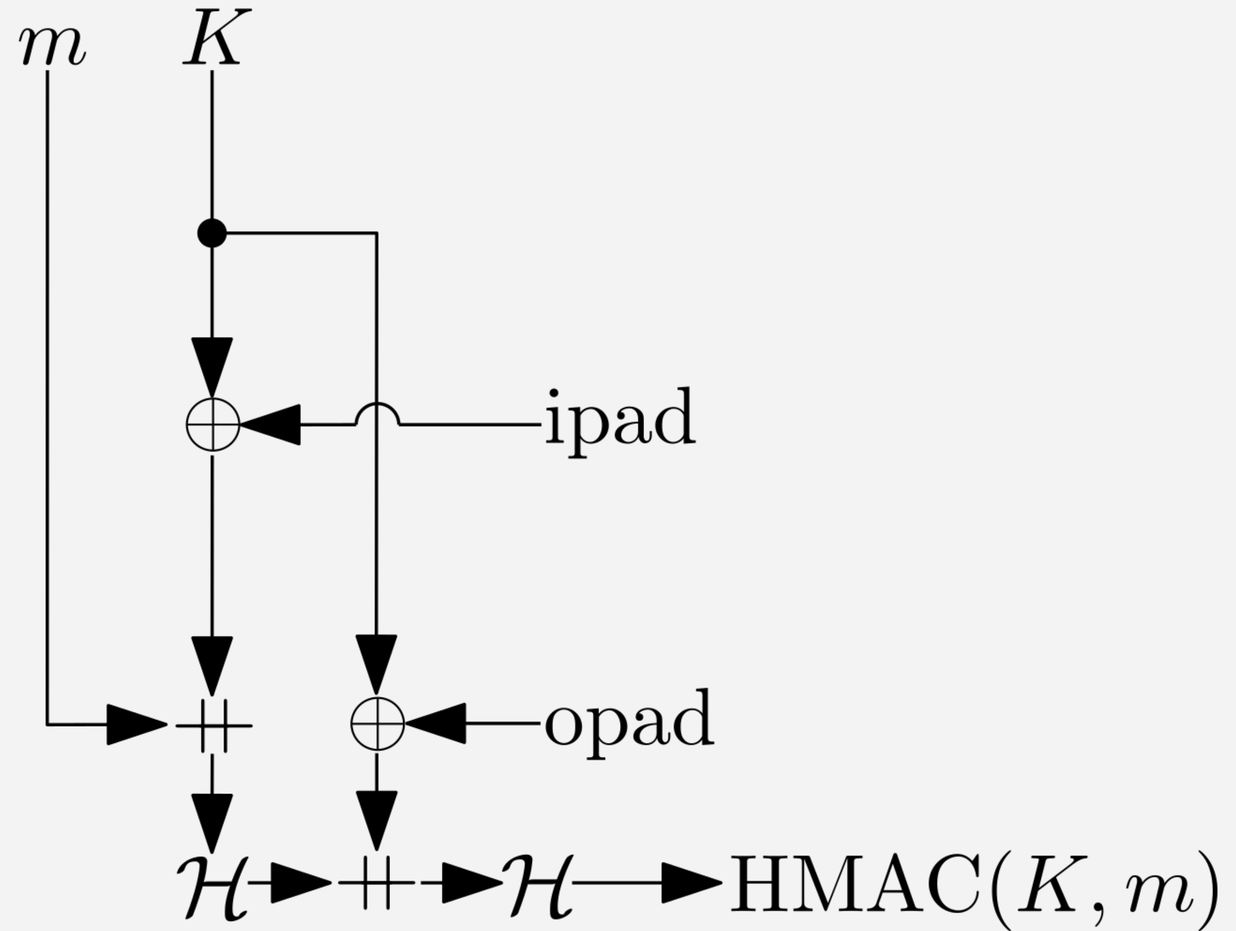
На основе хешей (HMAC)

На основе блочных шифров (например, CBC-MAC)

HMAC

HMAC =
 H((k ^ opad) || H((k ^ ipad) || m))

k - ключ
m - сообщение
opad, ipad - паддинги



Итоги

1. Назначение MAC
2. Виды MAC, пример уязвимой реализации
3. Устройство HMAC